Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) An electronic transaction verification system for use at a location where a transaction token is presented by an individual to complete a transaction comprising:

a transaction information database for storing an account information for an authorized user;

a first biometric database for storing biometric data for the authorized user;

a second biometric database for storing biometric data for a plurality of invalid users;

a reading device for reading the transaction token and transmitting transaction information data to the transaction information database;

a biometric data device for scanning and transmitting biometric data obtained with the transaction information data to the first biometric database;

wherein the biometric data device selectively transmits biometric data to the first biometric database for comparison with the biometric data

stored for the authorized user to verify the identity of the individual presenting the transaction token in real time;

wherein the biometric data is transmitted to the second biometric database to determine if the individual presenting the transaction token is an invalid user;

wherein the reading device selectively transmits transaction information data to the transaction information database for comparison with account information stored for the authorized user to verify a condition of the account to complete the transaction in real time; and

wherein a result from the comparisons with stored account information and stored biometric data for the authorized user is returned to the transaction location to accept or reject the transaction in real time.

2. (previously amended) The system of claim 1 further comprising:

a signature scanning device for scanning signature data received with the transaction information;

a signature database for storing signature data for the authorized user; and

wherein the signature scanning device selectively transmits signature data to the signature database for comparison with the signature stored for the authorized user in real time.

3. (original) The system of claim 1 wherein the transaction token comprises at least one of a check, a substitute check, a credit card, a debit card, a smart card, a promissory note, travelers check, and a food stamp.

4. (original) The system of claim 1 wherein the biometric data is any one of a fingerprint scan, retinal scan, an iris scan, a voice print, a hand geometry scan, or a facial scan.

5. (original) The system of claim 3 wherein the transaction information data includes data written in magnetic ink on the check.

6. (original) The system of claim 3 wherein the transaction information data includes data encoded on the transaction token.

7. (original) The system of claim 1 wherein the electronic transaction verification system selectively returns a report on customer usages.

8. (original) The system of claim 1 wherein the biometric data device further selectively encodes recorded biometric data on the transaction token.

9. (original) The system of claim 8 wherein the recorded biometric data is any one of a fingerprint scan, a retinal scan, an iris scan, a voice print, a hand geometry or a facial scan.

10. (original) The system of claim 1 wherein the reading device and the biometric data device are located remotely from the biometric database and the transaction information database.

11. (original) The system of claim 1 wherein the reading device and the biometric data device are located in proximity to the biometric database and the transaction information database.

12 - 13. (canceled)

14. (currently amended) An electronic transaction verification system for use at a location ~~were~~ where a transaction token is presented by an individual to complete a transaction, comprising:

a transaction information database for storing an account information for an authorized user;

a first biometric database for storing biometric data for the authorized user;

reading means for reading the transaction token and transmitting transaction information data to the transaction information database;

biometric data means for recording and transmitting biometric data received with the transaction information data to the first biometric database;

a second biometric database for storing biometric data for a plurality of invalid users;

wherein the reading means selectively transmits transaction information data to the transaction information database for comparison with account information for the authorized user to verify that the individual presenting the transaction token is the authorized user and to verify a condition of the account to complete the transaction in real time;

wherein the biometric data means selectively transmits biometric data to the first biometric database for comparison with the biometric data stored for the user to verify the identity of the individual presenting the transaction token in real time; ~~and~~

wherein the biometric data is transmitted to the second biometric database to determine if the individual presenting the transaction token is an invalid user; and

wherein a result from the comparisons with stored account information and stored biometric data for the authorized user is returned to the transaction location to accept or reject the transaction in real time.

15. (previously amended) The system of claim 14 further including:

signature scanning means for scanning signature data received with the transaction information;

a signature database for storing signature data for the authorized user; and

wherein the signature scanning means selectively transmits signature data to the signature database for comparison with the signature stored for the authorized user in real time.

16. (original) The system of claim 14 wherein the transaction token comprises at least one of a check, a substitute check, a credit card, a debit card, a smart card, a promissory note, a travelers check and a food stamp.

17. (original) The system of claim 16 wherein the transaction information data includes data written in magnetic ink on the check.

18. (original) The system of claim 16 wherein the transaction information data includes data encoded on the transaction token.

19. (original) The system of claim 14 further including report means for transmitting a report detailing customer usage of the electronic transaction verification system.

20. (original) The system of claim 14 further including means for selectively encoding the biometric data from the biometric data means in a readable medium on the transaction token.

21. (original) The system of claim 14 wherein the biometric data is any one of a fingerprint scan, a retinal scan, an iris scan, a voice print, a hand geometry scan, or a facial scan.

22 - 23. (canceled)

24. (currently amended) A method of verifying the identity of a person attempting to tender a transaction token to complete a transaction, and the condition of an account against which the transaction token is applied, the method comprising the steps of:

obtaining transaction information from the transaction token;

obtaining biometric data from the person tendering the transaction token;

selectively transmitting the transaction information to a transaction information database that stores an account information for an authorized user;

comparing the transmitted transaction information with the account information stored in the transaction information database to determine in real time if the account against which the transaction token is applied is in condition to ~~satisfy~~ complete the transaction and to verify that the individual presenting the transaction token is the authorized user;

selectively transmitting the biometric data to a first biometric database that stores biometric information for the authorized user;

comparing the transmitted biometric data with biometric information stored in the first biometric database to determine in real time if the person tendering the transaction token is authorized to use the account against which the transaction token is applied; ~~and~~

transmitting the biometric data to a second biometric database that stores biometric data for a plurality of invalid users;

comparing the transmitted biometric data with the biometric data stored in the second biometric database to determine if the individual presenting the transaction token is an invalid user; and

transmitting a result from the comparisons with stored account information and stored biometric data for the authorized user to a transaction location to accept or reject the transaction in real time.

25. (previously amended) The method of claim 24, further including the steps of:

obtaining the signature of the person tendering the transaction token;

selectively transmitting the signature information, either together with or separately from the transaction information and the biometric data, to a signature database that stores signature information for the authorized user;

comparing the transmitted signature information with signature information in the signature database to determine in real time if the signature is that of an authorized user for the account against which the transaction token is applied.

26. (original) The method of claim 24 further including the step of encoding the biometric data on the transaction token.

27. (original) The method of claim 24 further including the step of transmitting data indicative of whether the person is authorized to use the account to the location where the transaction information and biometric data are obtained.

28. (currently amended) An electronic transaction verification system for use with a transaction token processing system, at a location where a transaction token is presented by an authorized user to complete a transaction, comprising:

a reading device for reading the transaction token and transmitting transaction information to the transaction information database;

a first biometric data device for recording and transmitting biometric data that is received with the transaction token;

a second biometric database for storing biometric data for a plurality of invalid users;

a biometric database for storing biometric data for a plurality of authorized users;

a transaction information database for storing account information for an authorized user;

wherein the biometric device selectively transmits biometric data to the first biometric database to verify the identity of the individual presenting the transaction token in real time;

wherein the biometric data is transmitted to the second biometric database to determine if the individual presenting the transaction token is an invalid user;

wherein the reading device selectively transmits the transaction information to the transaction information database to verify the condition of the account to complete the transaction in real time and to verify that the individual presenting the transaction token is the authorized user; and

wherein a result from the comparisons with stored account information and stored biometric data for the authorized user is returned to the transaction location to accept or reject the transaction in real time.

29. (canceled)

30. (original) The electronic transaction verification system for use with a transaction token processing system of claim 28 wherein the transaction information comprises magnetic ink character recognition data that is printed on the negotiable instrument.

31. (original) The electronic transaction verification system for use with a transaction token processing system of claim 28 wherein the biometric data device digitizes a representation of the biometric data received with the transaction information and encodes the digitized biometric data directly on the transaction token.

32. (canceled)

33. (previously amended) The electronic transaction verification system for use with a transaction token processing system of claim 28 further comprising:

a scanning device for scanning signature data received with the negotiable instrument;

a signature database for storing signature data for the authorized user;

wherein the scanning device selectively transmits signature data to the signature database to determine in real time if the signature data was received from the authorized user.

34 – 37 (canceled)

38. (currently amended) A method for real time electronic verification and authorization of a transaction in which a token is presented to complete the transaction ~~for payment~~, comprising the steps of:

receiving transaction information from the token;

receiving biometric data from an individual who presented the token for payment;

comparing the received transaction information with account information stored for an authorized user ~~the individual~~ to determine if the account is in a satisfactory condition to complete the transaction and to verify that the individual presenting the transaction token is the authorized user;

comparing the received biometric data with biometric data stored for the ~~individual~~ authorized user to verify the identity of the individual presenting the token; ~~and~~

comparing the received biometric data with biometric data stored for a plurality of invalid users to determine if the individual presenting the token is an invalid user; and

authorizing the electronic transaction in real time if the account is in satisfactory condition and the identity of the individual is verified as the authorized user.

39. (previously presented) The method of claim 38 wherein the token comprises at least one of a check, a substitute check, a credit card, a debit card, a smart card, a promissory note, a traveler's check and a food stamp.

40. (previously presented) The method of claim 38 wherein the biometric data comprises at least one of a fingerprint scan, a retinal scan, an iris scan, a voice print, a hand geometry scan and a facial scan.

41. (currently amended) A method for real time electronic verification and authorization of a transaction in which a token is presented to complete the transaction ~~for payment~~, comprising the steps of:

receiving transaction information from the token;

receiving biometric data from an individual who presented the token for payment;

comparing the received transaction information with account information stored for ~~the individual~~ an authorized user to determine if the account is in a satisfactory condition to complete the transaction;

comparing the received biometric data with biometric data stored for ~~the individual~~ the authorized user to verify the identity of the individual presenting the token; ~~and~~

comparing the received biometric data with biometric data stored for a plurality of invalid users to determine if the individual presenting the token is an invalid user; and

rejecting the electronic transaction in real time if either the account is not in satisfactory condition or ~~the identity of~~ the individual is ~~not verified~~ determined to be an invalid user.

42. (previously presented) The method of claim 41 wherein the token comprises at least one of a check, a substitute check, a credit card, a debit card, a smart card, a promissory note, a traveler's check and a food stamp.

43. (previously presented) The method of claim 41 wherein the biometric data comprises at least one of a fingerprint scan, a retinal scan, an iris scan, a voice print, a hand geometry scan and a facial scan.